Legal Liability for Information System Security Compliance Failures: New Recipes for Electronic Sachertorte Algorithms

Panel Members, Affiliations and Statements

Fred Chris Smith, Trial Attorney in Private Practice in Santa Fe, New Mexico, Special Prosecutor and Computer Security Consultant

Fred Smith has practiced civil and criminal law in Colorado and New Mexico since graduating from Stanford Law School in 1972. He received a B. A. in philosophy from the University of Michigan. Fred served as the Director of Special Prosecutions and Investigations and as Director of Antitrust Enforcement for four New Mexico Attorneys General. In 1988-9 he served as the first Director of the National Association of Attorneys General RICO Enforcement Project in Washington D.C., which established special financial crime and civil litigation units in Arizona, Colorado, Oregon and Washington. Since 1985, he has developed and presented computer crime training programs for investigators and prosecutors throughout the United States. Since 1993, he has coordinated annual training conferences at Los Alamos National Laboratory in conjunction with SEARCH and the New Mexico High Tech Crime Investigation Association, for law enforcement and corporate security professionals, providing intermediate and advanced training in computer security policies and procedures, and Internet crime detection and prosecution.

John Montjoy, Sr. VP and General Counsel, BBN Corporation

John Montjoy is the Senior Vice President and General Counsel of BBN Corporation, the leading independent provider of Internet services. He graduated from Tulane University Law School in 1969 and joined BBN as General Counsel in 1984. His responsibilities include all legal, regulatory and contractual affairs of the company. Before joining BBN he was in the legal department of Signal Cos., Cincinnati Milacron and Schlumberger Ltd. John has more than 25 years experience in computer law and continues to be very active in the formation of law and in solving legal problems related to the Internet. He was a founder of the Internet Law and Policy Forum, a not-for-profit non-governmental organization composed of approximately thirty leading Internet companies around the world. He currently serves on the executive committee of the Forum.

Edward Tenner, Writer and Visiting Researcher in the Department of Geological and Geophysical Sciences at Princeton University

Edward Tenner was formerly the executive editor for physical science and history at Princeton University Press. In 1995-6 he was a Fellow of the Woodrow Wilson International Center for Scholars served as a consultant to the Jerome and Dorothy Lemelson Center for the History of Invention and Innovation, National Museum of American History, Smithsonian Institution to select inventors whose work will be documented and studied. He received an A.B, from

Princeton and his Ph.D. in history from the University of Chicago. He has held visiting research positions at Rutgers University and the Institute for Advanced Study. In 1996, his book, Why Things Bite Back: Technology and the Revenge of Unintended Consequences, was published by Alfred Knopf.

David J. Loundy, Internet Service Provider Attorney in Private Practice in Highland Park, Illinois, and an Electronic Publisher of His Own Computer Law Related Articles

David Loundy practices law in the Chicago area and provides legal representation to ISPs and other clients with on-line content legal issues. He graduated with distinction from Purdue University with a B.A. in Telecommunications. He received his J.D. with distinction from the University of Iowa College of Law. David has published a number of articles on a wide range of computer related legal topics. He writes a monthly column on *Technology Law* for the Chicago Daily Law Bulletin and a monthly column appearing in The Cyberspace Lawyer entitled, *E-Law*. In 1993 and 1994 he published articles on computer information system law and system operator liability in the E-Law Journal, the Albany Law Journal of Science & Technology and Computer/Law Journal. His article, *Revising the Copyright Law for Electronic Publishing*, was published in the John Marshall Journal of Computer and Information Law in 1995. He is currently Vice-chair of the Chicago Bar Association Computer Law Committee. Some of his articles can be found on-line at http://www.Loundy.com/

Panel Summary

The rapid growth in computer network technology and on-line services continues to generate a dramatic increase in the number of networks and in the number and variety of users of these electronic communications services. Computer network security has lagged behind the implementation of new and increasingly complex computer systems. As more and more services are demanded and used by more and more people and institutions, there are more and more ways that things can go and do go wrong, which in turn give rise to consequences offending or injuring the interests or the assets of individuals and businesses. One factor which has not been given sufficient consideration, but which could become extremely important in the equation of how to go about improving the safety and security of network computing, is the obvious conclusion that a large number of lawyers are rapidly becoming computer literate and will sooner or later be ready, willing and able to assist new claimants, who are or soon will be aware of potential legal claims for the violation of their real or imagined rights, damages to their interests and real or virtual injuries, in developing new causes of action for courts to consider, all based on computer network security failures or shortcomings.

John Montjoy will give the viewpoint of a large Internet Service Provider in discussing the current legal and regulatory environment surrounding the Internet and several aspects of information system protection hardware, software and security practices and procedures.

Drawing on some of the material collected in his recently published book, Why Things Bite Back: Technology and the Revenge of Unintended Consequences, Ed Tenner will develop one

or two historical technological analogies, such as the developments in medicine or the transportation industry, which gave rise to a great deal of tort litigation, as examples of how the rapid development of new technologies and the wide-spread use of them has ineluctably led to a dramatic increases in tort liability for injured claimants. Sound information system security standards and procedures can be seen to incorporate some of the same lessons which can be learned from the study of new technology adoption and litigation explosion spirals of other evolving technologies. Based on those histories, the constant upgrading of system monitoring and attention to detail will be required to take full advantage of new security technologies, while helping to reduce the number of unfortunate accidents or risks of catastrophe. Dr. Tenner will attempt to apply the lessons learned from his historical study to the problems arising from the intensification of computer networking and some predictable failures and injuries arising from the lack of compliance with adequate computer network security administrator precautions or user vigilance.

David Loundy will summarize the cases that have attempted to impose legal liability on service providers and sysadmins and then generalize from those cases about what we might expect to see as the contract and tort bars and their respective good and bad faith claimants begin to see or at least to smell the virtual blood. David will take a step into the future and discuss some of the legal problems that security systems based on encryption schemes and various systems management policies may create in the form of privacy violations for negligent disclosures, or breach of contract allegations by third parties for lost information when current or past employees can't or won't decrypt keyed information. Potential liability issues involving denial of service due to security precautions will be considered.

Fred Chris Smith will moderate the panel discussion. Drawing on his background as a litigator and as a criminal prosecutor of financial fraud and civil RICO enforcement actions involving complex criminal schemes, he will suggest that our telecommunication miracles will be just as valuable for criminal enterprises as they have proven to be for legitimate businesses. Given the almost perfect vacuum of law enforcement capabilities currently available to deal with this growing criminal problem, there is apt to be even greater pressure placed upon the traditional alternatives to criminal enforcement of financial fraud and other white collar crimes, through increased regulation and civil litigation in one form or another. In this chaotic transition from the relatively secure MIS based corporate information to open systems and global networks, legal standards are being established by negotiation, custom or by jury verdict, rather than by legislation and enforced by regulation or police action. In such a world, it is most likely that the major deterrents to attacks on network security systems will not come from public law enforcement agencies, but will be privately orchestrated and pursued, in part through an increased number of civil law suits. In the absence of a clear set of legal standards of right and wrong and lacking any reasonably certain punishment meted out by the criminal justice system, it may prove difficult for system administrators and attorneys alike to draw clear lines between unjustified civil suits based on phantom risks, and the kinds of negligent failures to comply with generally recognized standards for adequate security precautions, which should give rise to legal liability and claims for damages.

Time will be made available between presentations and at the conclusion of the discussion among the panel members for written and oral questions from the audience.